iptables firewall configuration

Tutorial pdfs

This lab is divided into six different pdf documents and few web pages. This is basic information document. You can read the other tutorial documents and web pages in this order:

1. `iptables.pdf`
2. `Limiting_number_of_simultaneous_connections.pdf`
3. `Rate_limiting_using_iptables.pdf`
4. `Limiting_number_of_new_connections.pdf`
5. `NAT_using_iptables.pdf`
6. http://www.debian-administration.org/articles/268 - Port knocking using default iptables modules
7. http://www.cipherdyne.org/fwknop/docs/SPA.html - Understand single packet authorization
8. http://www.cipherdyne.org/fwknop/ - Single packet authorization and port knocking
9. http://portknocko.berlios.de/README.html - iptables extension for port knocking
10. http://www.portknocking.org/ - List of resources / implementations related to port knocking
11. http://lebelt.info/old/?item=webknocking_en - Web knocking
12. http://en.gentoo-wiki.com/wiki/Port_Knocking - Port knocking daemon

13. http://www.netfilter.org/projects/patch-o-matic/pom-external.html - pknock iptables port knocking module

14. http://www.hauntednipple.co.uk/?p=67 - knockd daemon configuration example

Two teams can work together in this lab to perform tasks mentioned in the tutorial pdfs and web pages.

Lab tasks

1. Start web server, ftp server, ssh server etc. on both machines and try to ping, connect to all started servers on both machines.

2. Try to secure your server as much as possible based on learned techniques.

Submission

Each group of two teams must submit very good firewall configuration that protects the machine on or before 5th October, 2011 evening 05:00pm.

You should submit two ideal configurations one for iptables and other for ip6tables. Both files should be properly commented and can include reasoning why particular port/protocol is allowed blocked/etc.

You can use port knocking, web knocking and single packet authorization techniques for protection. But in that case you should submit their configuration and steps on how to access particular service like SSH.